IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

STEVEN TEPPLER, individually and on behalf of all others similarly situated, Plaintiff, v. **TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Steven Teppler, individually and on behalf of all others similarly situated, brings this action against Teachers Insurance and Annuity Association of America ("TIAA"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold TIAA responsible for the injuries TIAA inflicted on Plaintiff and approximately 2.4 million similarly situated persons ("Class Members") due to TIAA's impermissibly inadequate data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by

cybercriminals (the "Data Breach" or "Breach") on May 29, 2023.[1] Upon information and belief, the cybercriminals who perpetrated the Breach are part of the Clop crime group.[2]

2. The data that TIAA caused to be exfiltrated by cybercriminals were highly sensitive. Upon information and belief, the exfiltrated data included personal identifying information ("PII") like individuals' names and Social Security numbers.

3. Upon information and belief, prior to and through the date of the Data Breach, TIAA obtained Plaintiff's and Class Members' PII and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, TIAA inadequately maintained its network, platform, software, and technology partners—rendering these easy prey for cybercriminals.

4. Upon information and belief, the risk of the Data Breach was known to TIAA. Thus, TIAA was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

5. Then, after the Data Breach, TIAA failed to provide timely notice to the affected Plaintiff and Class Members—thereby exacerbating their injuries. Ultimately, TIAA deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, TIAA impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

---

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/ed67df63-aced-4ecb-91ce-602c7e34c83a.shtml (last accessed on August 22, 2023).

[2] https://www.bankinfosecurity.com/latest-moveit-data-breach-victim-tally-455-organizations-a-22650 (last accessed on July 26, 2023).

6. Even when TIAA finally notified Plaintiff and Class Members of their PII's exfiltration, TIAA failed to adequately describe the Data Breach and its effects.

7. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of TIAA's negligence. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

8. Armed with the PII stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

9. And Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII were exfiltrated and compromised in the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to TIAA's data security systems, future annual audits, and adequate credit monitoring services funded by TIAA.

PARTIES

13. Plaintiff Teppler is a natural person and citizen of Florida, residing in Jacksonville, Florida. He has no intention of moving to a different state in the immediate future.

14. Defendant is a not for profit corporation with its headquarters and principal place of business at 730 Third Avenue, New York, New York 10017.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because many members of the class are citizens of states different than that of TIAA.

16. This Court has general personal jurisdiction over TIAA because TIAA's principal place of business and headquarters is in this District. TIAA also regularly conducts substantial business in this District.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and TIAA conducts substantial business in this District.

FACTUAL ALLEGATIONS

TIAA Collected and Stored the PII of Plaintiff and Class Members

18. Defendant is a Fortune 100 financial services organization that provides financial services in the academic, research, medical, cultural and governmental fields.

19. TIAA serves over 5 million active and retired employees participating at more than 15,000 institutions and has $1 trillion in combined assets under management with holdings in more than 50 countries (as of December 31, 2017).

20. Upon information and belief, TIAA received and maintained the PII of Plaintiff and Class Members (through its website and otherwise), such as individuals' names and Social Security numbers. These records are stored on TIAA's and its partners' computer systems.

21. Upon information and belief, TIAA received the PII of Plaintiff and Class Members' from TIAA's customers for whom TIAA administers financial services.

22. Upon information and belief, TIAA directly or indirectly used Progress Software Corporation ("PSC") for information technology management and software

services, including PSC's file transfer software, MOVEit. Within this relationship, TIAA transferred and entrusted data, including Plaintiff's and Class Members PII, to PSC.

23. Upon information and belief, PSC's file transfer software, MOVEit, was hacked by the Clop crime group, resulting in the Breach and the exfiltration of customer PII, including Plaintiff's and Class Members PII.

24. Because of the highly sensitive and personal nature of the information TIAA acquires and stores, TIAA knew or reasonably should have known that it stored protected PII and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' PII and provide adequate notice to customers if their PII is disclosed without proper authorization.

25. When TIAA collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

26. TIAA acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII.

27. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII, TIAA assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

28. On TIAA's website, TIAA represents that, "We at TIAA are committed to protecting your privacy in accordance with the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the

Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), applicable state laws and this privacy notice."[3]

29. On TIAA's website, TIAA represents that, "TIAA protects the personal information you provide against unauthorized access, disclosure, alteration, destruction, loss, or misuse. Your personal information is protected by physical, electronic, and procedural safeguards in accordance with federal and state standards. These safeguards include appropriate procedures for access and use of electronic data, provisions for the secure transmission of sensitive personal information on our website, and telephone system authentication procedures. Additionally, we limit access to your personal information to those TIAA employees and agents who need access in order to offer and provide products or services to you. We also require our service providers to protect your personal information by utilizing the privacy and security safeguards required by law."[4]

30. Upon information and belief, TIAA represented to its customers and the public orally, in written contracts, marketing materials, and otherwise that it would properly protect all PII it obtained. Upon information and belief, TIAA knew or reasonably should have known that these representations would be transmitted to the public, including Plaintiff and Class Members.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and

[3] https://www.tiaa.org/public/support/privacy/privacy-notice.
[4] *Id.*

passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

32. Upon information and belief, Plaintiff and Class Members relied on TIAA to keep their PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

33. TIAA could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners.

34. TIAA's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

35. Despite the prevalence of public announcements of data breaches and data security compromises, TIAA failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

36. TIAA failed to properly select its information security partners.

37. TIAA failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

38. TIAA failed to ensure the proper monitoring and logging of file access and modifications.

39. TIAA failed to ensure the proper training of its technology partners' employees as to cybersecurity best practices.

40. TIAA failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

41. TIAA failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

42. TIAA knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

43. TIAA failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and potentially disclose it to others without consent.

44. Upon information and belief, TIAA failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

45. Upon information and belief, TIAA failed to ensure the proper encryption of Plaintiff's and Class Members' PII and monitor user behavior and activity to identify possible threats.

The Data Breach

46. On or about July 14, 2023, TIAA notified the public ("Notice of Data Breach" or "Notice") that its customers' data had been compromised in a Data Breach suffered by PSC and PBI, and informed them of the following:

> Pension Benefit Information, LLC ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including Teachers Insurance and Annuity Association of America ("TIAA"). PBI is

providing notice of a third-party software event that may affect the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, address, and gender.[5]

47. Upon information and belief, the Notice of Data Breach was drafted and publicized under the direction of PSC, PBI, and TIAA.

48. Upon information and belief, TIAA has sufficient control over its data which was stored and/or transported over PSC's file transfer software, MOVEit to properly secure that data.

49. Upon information and belief, Plaintiff's and Class Members' affected PII was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/ed67df63-aced-4ecb-91ce-602c7e34c83a/6319b5c9-ea99-46c6-a763-aa258e5fd897/document.html.

50. It is likely the Data Breach was targeted at PSC due to its status as large information technology provider to businesses that collect, create, and maintain PII.

51. TIAA was unreasonably delayed in providing notice of the Breach to Plaintiff and Class Members.

52. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

53. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, TIAA advised impacted individuals to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors" and to:

a. order your free credit report;

b. if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the FTC and/or your

state's attorney general office about for information on how to prevent or avoid identity theft;

c. place a security freeze; and

d. place a fraud alert.[6]

54. TIAA largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

55. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[7]

56. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[8] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[9] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating

---

[6] *Id.*

[7] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[8] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

[9] *Id.*

with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

57. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

58. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

59. TIAA also offered credit monitoring services for a period of 24 months. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for their respective lifetimes.

60. TIAA had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

61. TIAA's Breach Notice letter, as well as its website notice, both omit the size and scope of the breach. TIAA has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

62. Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular ransomware used, and what steps are being

taken, if any, to secure their PII and financial information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly TIAA intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

63. Plaintiff's and Class Members' PII and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and financial information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

TIAA Failed to Comply with FTC Guidelines

64. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[10] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as TIAA, should employ to protect against the unlawful exfiltration of PII.

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[11] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

[10] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed July 25, 2022).
[11] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed July 25, 2022).

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

66. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

67. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[12]

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. TIAA's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

[12] *See Start with Security*, *supra* note 46.

TIAA Failed to Follow Industry Standards

70. Despite its alleged commitments to securing sensitive data, TIAA does not follow industry standard practices in securing PII.

71. Experts studying cyber security routinely identify financial service providers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

72. Several best practices have been identified that at a minimum should be implemented by financial service providers like TIAA, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

73. Other best cybersecurity practices that are standard in the financial service industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

74. TIAA failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all

established standards in reasonable cybersecurity readiness.

75. Such frameworks are the existing and applicable industry standards in the financial service industry. And TIAA failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

The Experiences and Injuries of Plaintiff and Class Members

76. Plaintiff and Class Members are financial services customers of TIAA's customers.

77. As a prerequisite of receiving its services, TIAA requires its customers to disclose the PII of Plaintiff and Class Members.

78. When TIAA finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. TIAA's Breach Notice fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

79. Because of the Data Breach, TIAA inflicted injuries upon Plaintiff and Class Members. And yet, TIAA has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

80. All Class Members were injured when TIAA caused their PII to be exfiltrated by cybercriminals.

81. Plaintiff and Class Members entrusted their PII to TIAA. Thus, Plaintiff had the reasonable expectation and understanding that TIAA would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from

unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff would not have entrusted their PII to TIAA had they known that TIAA would not take reasonable steps to safeguard their information.

82. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that TIAA obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

83. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

84. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

85. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff Teppler's Experience

86. Plaintiff Teppler's employer's retirement plan was administered by TIAA.

87. Plaintiff Teppler first learned of the Breach when he received a notice via mail (substantially similar to the Notice) from Defendant sometime on or around August 15, 2023, which informed him that his PII, including his Social Security number and date of birth, was compromised in the Breach.

88. Shortly after and as a result of the Data Breach, Plaintiff Teppler experienced an increase in spam and suspicious phone calls, texts, and emails.

89. As a result of the Data Breach and at the recommendation of TIAA and its Notice, Plaintiff Teppler made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing financial statements.

90. Plaintiff Teppler has spent a significant amount of time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

91. Plaintiff Teppler suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and/or financial information.

92. Plaintiff Teppler is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII and financial information, in combination with his names, being placed in the hands of unauthorized third parties/criminals.

93. Plaintiff Teppler has a continuing interest in ensuring that his PII and

financial information, which, upon information and belief, remains backed up in TIAA's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

94. Plaintiff and Class Members suffered injury from the misuse of their PII that can be directly traced to TIAA.

95. The ramifications of TIAA's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

96. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[13]

97. As a result of TIAA's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

[13] *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of TIAA and is subject to further breaches so long as TIAA fails to undertake the appropriate measures to protect the PII in their possession.

98. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[14]

[14] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

99. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

100. It can take victims years to spot or identify PII theft, giving criminals plenty of time to milk that information for cash.

101. One such example of criminals using PII for profit is the development of "Fullz" packages.[15]

102. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

103. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other

[15] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

104. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

105. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." TIAA did not rapidly report to Plaintiff and the Class that their PII had been stolen.

106. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

107. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports

and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

108. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

109. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[16]

110. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[17] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on

---

[16] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[17] *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 21, 2022).

networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[18]

111. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[19] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the "FTCA").

112. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[TIAA] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[TIAA] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and

[18] *Id.*
[19] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen.

"failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[TIAA] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. TIAA thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

113. Charged with handling highly sensitive PII including, financial information, and insurance information, TIAA knew or should have known the importance of safeguarding the PII that was entrusted to it. TIAA also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on TIAA's customers' as a result of a breach. TIAA nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

114. TIAA disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, TIAA opened, disclosed, and failed to adequately protect the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

115. TIAA's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

116. TIAA's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

117. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

118. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons residing in the United States whose PII was impacted by the Data Breach—including all persons that received a Notice of the Data Breach (the "Class").

119. The Class defined above is readily ascertainable from information in TIAA's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

120. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) TIAA, TIAA's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which TIAA or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and TIAA's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

121. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

122. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

123. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of the approximately two million individuals whose PII were compromised by TIAA's Data Breach.

124. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If TIAA unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If TIAA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If TIAA's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If TIAA's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If TIAA owed a duty to Class Members to safeguard their PII;

f. If TIAA breached its duty to Class Members to safeguard their PII;

g. If TIAA knew or should have known that its data security systems and monitoring processes were deficient;

h. If TIAA should have discovered the Data Breach earlier;

i. If TIAA took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If TIAA's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If TIAA's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If TIAA's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of TIAA's misconduct;

o. If TIAA breached implied contracts with Plaintiff and Class Members;

p. If TIAA was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If TIAA failed to provide notice of the Data Breach in a timely manner; and

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

125. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to TIAA's uniformly illegal and impermissible conduct.

126. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

127. **Predominance**. TIAA has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way.

The common issues arising from TIAA's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

128. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for TIAA. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

129. The litigation of the claims brought herein is manageable. TIAA's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

130. Adequate notice can be given to Class Members directly using information maintained in TIAA's records.

131. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of

which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 121.

132. TIAA has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

133. Plaintiff re-alleges and incorporate by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

134. TIAA required its customers Plaintiff and Class Members to submit Plaintiff's and Class Memberss non-public PII to TIAA to receive TIAA's services.

135. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, TIAA owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. TIAA's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

136. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that TIAA holds vast amounts of PII, it was inevitable that unauthorized individuals would at some point try to access TIAA's databases of PII.

137. After all, PII is highly valuable, and TIAA knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, TIAA knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

138. TIAA owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

139. TIAA's duty of care to use reasonable security measures arose because of the special relationship that existed between TIAA and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. TIAA was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

140. TIAA failed to take appropriate measures to protect the PII of Plaintiff and the Class. TIAA is morally culpable, given the prominence of security breaches in the financial service industry. Any purported safeguards that TIAA had in place were wholly inadequate.

141. TIAA breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII.

142. The failure of TIAA to comply with industry and federal regulations evinces TIAA's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

143. But for TIAA's wrongful and negligent breach of their duties to Plaintiff and the Classes, Plaintiff's and Class Members' PII would not have been compromised, stolen, and viewed by unauthorized persons. TIAA's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Classes and all resulting damages.

144. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of TIAA's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. TIAA knew or should have known that their systems and technologies for processing and securing the PII of Plaintiff and the Classes had security vulnerabilities.

145. As a result of this misconduct by TIAA, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII being disclosed to third parties without the consent of Plaintiff and the Classes

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

146. Plaintiff re-alleges and incorporate by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

147. Under the Federal Trade Commission Act, TIAA had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or

affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[20]

148. Moreover, Plaintiff and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that TIAA inflicted upon Plaintiff and Class Members.

149. TIAA's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because TIAA are bound by industry standards to protect confidential PII.

150. TIAA owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to their PII. TIAA also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of TIAA's Data Breach.

151. TIAA owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom TIAA knew or should have known would suffer injury-in-fact from its inadequate security

[20] 15 U.S.C. § 45.

protocols. After all, TIAA actively sought and obtained the PII of Plaintiff and Class Members.

152. TIAA breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. And but for TIAA's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by TIAA include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—FTCA and its regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

153. It was foreseeable that TIAA's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and

data breaches in the financial service industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

154. Simply put, TIAA's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by TIAA's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

155. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

156. Plaintiff and Class Members are also entitled to injunctive relief requiring TIAA to, *e.g.,* (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

157. Plaintiff re-alleges and incorporate by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

158. This cause of action is plead in the alternative to the breach of implied contract theory.

159. Plaintiff and Class Members conferred a monetary benefit on TIAA, by paying money for services, a portion of which was intended to have been used by TIAA for data security measures to secure Plaintiff and Class Members' PII. Plaintiff and Class Members further conferred a benefit on TIAA by entrusting their PII to TIAA from which TIAA derived profits.

160. TIAA enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, TIAA instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of TIAA's failure to provide adequate security.

161. Under the principles of equity and good conscience, TIAA should not be permitted to retain the money belonging to Plaintiff and Class Members, because TIAA failed to implement appropriate data management and security measures that are mandated by industry standards.

162. TIAA acquired the monetary benefit, PII, and PHI through inequitable means in that TIAA failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

163. If Plaintiff and Class Members knew that TIAA had not secured their PII, they would not have agreed to give their money—or disclosed their data—to TIAA or TIAA's customers.

164. Plaintiff and Class Members have no adequate remedy at law.

165. As a direct and proximate result of TIAA's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII, which remain in TIAA's possession and is subject to further unauthorized disclosures so long as TIAA fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of TIAA's Data Breach.

166. As a direct and proximate result of TIAA's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

167. TIAA should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
Violations of New York General Business Law,
N.Y. Gen. Bus. Law §§ 349, *et seq*.
(On Behalf of Plaintiff and the Class)

168. Plaintiff re-alleges and incorporate by reference paragraphs 1-132 of the Complaint as if fully set forth herein.

169. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

170. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

171. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and Class Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

172. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as

described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

173. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Defendant Data Breach.

174. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid.

175. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and the undersigned as Class counsel;

B. A mandatory injunction directing TIAA to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

   i. prohibiting TIAA from engaging in the wrongful and unlawful acts

described herein;

ii. requiring TIAA to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring TIAA to delete and purge the PII of Plaintiff and Class Members unless TIAA can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring TIAA to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. requiring TIAA to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on TIAA's systems on a periodic basis;

vi. prohibiting TIAA from maintaining Plaintiff's and Class Members' PII on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring TIAA to segment data by creating firewalls and access controls so that, if one area of TIAA's network is compromised, hackers cannot gain access to other portions of TIAA's systems;

viii. requiring TIAA to conduct regular database scanning and securing checks;

ix. requiring TIAA to monitor ingress and egress of all network traffic;

x. requiring TIAA to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xi. requiring TIAA to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with TIAA's policies, programs, and systems for protecting personal identifying information;

xii. requiring TIAA to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor TIAA's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring TIAA to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that TIAA provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. Enjoining TIAA from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: August 31, 2023

Respectfully Submitted,

/s/ Jonathan M. Sedgh
Jonathan M. Sedgh

MORGAN & MORGAN
850 3rd Ave, Suite 402
Brooklyn, NY 11232
Phone: (212) 738-6839
Fax: (813) 222-2439
Email:jsedgh@forthepeople.com

Tim Semelroth
tsemelroth@fightingforfairness.com
RSH LEGAL
425 Second Street SE, Suite 1140
Cedar Rapids, IA 52401
T: 319-365-9200
F: 319-365-1114

John A. Yanchunis*
JYanchunis@forthepeople.com
Ra O. Amen*
Ramen@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Class